UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/718,175	11/19/2003	**Preetham Kajekar**	50325-0817	9355

29989 7590 06/21/2010

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
CHEA, PHILIP J	

ART UNIT	PAPER NUMBER
2453	

MAIL DATE	DELIVERY MODE
06/21/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/718,175	KAJEKAR ET AL.	
	Examiner	Art Unit	
	PHILIP J. CHEA	2453	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,15-39,41-62 and 64-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,15-39,41-62 and 64-72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to an Amendment filed 3/15/10. Claims 1-13,15-39,41-62 and 64-72 are currently pending. Any rejection not set forth below has been overcome by the current Amendment.

Claim Objections

1. Claims 49-71 objected to because of the following informalities: The "computer-readable storage medium" may be construed by one of ordinary skill in the art as a signal or transmission medium. In order to keep the claim statutory, the Examiner suggest amending the claim to read "A non-transitory computer-readable storage medium". Appropriate correction is required.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (US 2005/0193430), herein referred to as Cohen, and further in view of Milliken et al. (US 7,200,105), herein referred to as Milliken. The Examiner is relying on the parent application filing date of Cohen (10/1/02) to antedate the filing date of the instant application.

As per claims 25,1,22,25-27,49,72, Cohen discloses a method of determining network penetration, the method comprising the computer-implemented steps of:

representing a travel of a packet in a network based on topology data and on security policy data including at least

defining a packet by at least specifying a source address, an entry port and a destination port;

starting a loop for a current network device (see paragraphs 34-35 an paragraph 69, *it is implied that the packet must travel through a source address and entry and destination port,* and paragraph 75, *showing various ports that the packets may traverse*);

accessing access control list (ACL) data stored in an ACL database and the topology data stored in a topology database (see paragraph 28);

deciding whether an ingress interface of a current network device allows entry into the current network device, if the entry is not permitted, then terminating the loop for the current network device, if the entry is permitted continuing the loop, then performing the steps of checking one or more outbound ACLs for each outbound interface of the current network device to determine one or more possible outbound interfaces on which egress of the packet is permitted (see paragraph 35 and paragraph 47);

based on topology data, determining if there are any neighboring network device that are connected to the one or more possible outbound interfaces on which the egress of the packet is permitted from the current network device (see paragraph 37), if there are not any neighboring network devices, then an indication of the current network device is returned as a maximum penetration point as at least part of results of the step of representing, and the loop is terminated; if there is a neighboring network device, then the loop continues determining whether or not there are any remaining outbound interfaces for which results of a possible egress of the packet have not been determined, if there are no more remaining outbound interfaces, the loop is terminated, if there are more remaining interfaces, then the current network device is set to the neighboring network device to corresponding one of the remaining outbound interfaces, and if the loop has not been terminated for the current network device, restarting the loop for the current network device (see paragraph 48, *discussing traversing the topology of the network node by neighboring node as long as the attack can continue, and stopping until an attack can no longer be sustained because the constraint of the attack at the current node is not met or it has run out of nodes to continue*).

In considering the displaying of the graph, Cohen discloses that the attack graph (path of packet travel while penetrating the network is displayed in graph form (see paragraph 30).

Although the system disclosed by Cohen shows substantial features of the claimed invention (discussed above), it fails to disclose determining if the static routing table is present then determining to which interface outbound traffic is permitted to exit, and if the static routing table is not present, then allowing outbound traffic to exit through all outbound interfaces.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Cohen, as evidenced by Milliken.

In an analogous art, Milliken discloses a system for point of ingress traceback of a network attack (see Title). Milliken discloses that a router may include multiple input interfaces and routing tables that may determine the active route to network destinations (see column 4, lines 47-59). Milliken further discloses determining if a static routing table is present, if the static routing table is present then determining to which interface outbound traffic is permitted to exit, and if the static routing table is not present, then allowing outbound traffic to exit through all outbound interfaces (see column 4, lines 40-65).

Given the teaching of Milliken, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Cohen by employing a determination of a static routing table, such as disclosed by Milliken, in order to gather information about the path of packet travel that is allowed through a router.

As per claims 2,28,50, Cohen discloses wherein the security policy data comprises one or more access control lists of one or more network devices in the network (see paragraph 35).

As per claims 3,29,51, Cohen, further comprising the step of receiving packet parameters (see paragraph 35).

As per claims 4,30,52, Cohen discloses wherein the packet parameters comprise the network entry point where the packet enters the network (see paragraph 35).

As per claims 5,31,53, Cohen discloses wherein the packet parameters comprise a destination address (see paragraph 35).

As per claims 6,32,55, Cohen discloses wherein the topology data is received as input related to a user interface (see paragraph 57).

As per claim 7,33,56, Cohen discloses wherein the security policy data is based on access control lists associated with input received in a user interface (see paragraph 11).

As per claims 8,34,57, Cohen discloses further comprising determining a maximum penetration point (see paragraph 47).

As per claims 9,35,58, Cohen discloses wherein the step of representing comprises accessing the security policy data and the topology data related to a neighbor network device for which it has been determined that the packet could reach (see paragraph 35).

As per claims 10,36,59, Cohen discloses wherein the step of representing comprises determining whether ingress is allowed to a neighbor network device for which it has been determined that the inbound interface could be reached by the packet (see paragraph 35).

As per claims 11,37,60, Cohen discloses wherein the step of representing comprises determining whether there are any neighboring network devices to a neighbor network device for which it has been determined that the packet could reach (see paragraph 37).

As per claims 12,38,61, Cohen discloses wherein the step of representing comprises determining

whether there are any outbound interfaces that have not yet been checked for whether there is another network device connected thereto (see paragraph 36).

As per claims 13,39,62, Cohen discloses wherein the step of representing comprises recursively applying the step of determining whether there are any outbound interfaces (see paragraph 47).

As per claim 15,41,64, Cohen discloses receiving packet parameters specifying information corresponding to a plurality of packets (see paragraph 35).

As per claims 16,23,42,65, Milliken discloses wherein the step of representing comprises: for a neighbor network device for which it is determined that the packet could reach, determining if a static routing table is present; and if the static routing table is present, then accessing the static routing table, and determining an outbound interface through which egress of the packet is permitted based on the static routing table (see column 4, lines 40-65).

As per claims 17,24,43,66, Cohen discloses not considering outbound interface through which egress of the packet is permitted by the static routing table but is not permitted by an access control list associated with the security policy data (see paragraph 35).

As per claims 18,44,67, Milliken discloses wherein the step of representing comprises: for a neighbor network device for which it is determined that the packet could reach, determining if a static routing table is present; and if the static routing table is not present, then for each outbound interface of the neighbor
network device, representing an egress by the packet as part of the representing of the travel of the packet (see column 4, lines 40-65).

As per claims 19,45,68, Cohen further discloses receiving packet parameters that support

transmission control protocol flags (see paragraph 75, *showing transmission control protocol ports i.e. FTP, implying the support of flags*).

As per claims 20,46,69, Cohen discloses wherein the results comprise a graphical display of at least allowed paths of the packet (see paragraph 30).

As per claim 47,70, Cohen further discloses mapping of network devices and connections between the network devices (see paragraph 34).

As per claims 48,71, Cohen discloses the steps claimed because all inbound interfaces and outbound interfaces are scanned according to ACLs and also their neighboring endpoints until no more endpoints are available for checking (see paragraph 35).

As per claim 54, Cohen further discloses reading topology information from a topology database (see paragraph 48).

Response to Arguments

3. Applicant's arguments filed 3/15/10 have been fully considered but they are not persuasive.

A) Applicant contends that Cohen does not disclose checking inbound ACLs and outbound ACLs of network device interfaces.

In considering A), the Examiner respectfully disagrees. Cohen makes it clear that all ACLs are checked by network discovery agents including those for all inbound and outbound IP traffic which represent the possible starting points for an attack on the network (see paragraph 35).

B) Applicant contends that Cohen determines whether an attacker can obtain access to nodes in the network, and not for the purpose of determining whether a packet can travel to a given node.

In considering B), the Examiner respectfully disagrees. Cohen explicitly states analyzing attack routes i.e. path of travel for an attack (see paragraph 34).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHILIP J. CHEA whose telephone number is (571)272-3951. The examiner can normally be reached on M-F 6:30-4:00 (1st Friday Off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on 571-272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Philip J Chea
Primary Examiner
Art Unit 2453

/Philip J Chea/
Primary Examiner, Art Unit 2453
6/17/10